APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/678,936	10/03/2003	David Andrew Thomas	200309085-1	1203

22879   7590   06/23/2008
HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER
DINH, MINH

ART UNIT	PAPER NUMBER
2132	

NOTIFICATION DATE	DELIVERY MODE
06/23/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
mkraft@hp.com
ipa.mail@hp.com

United States Patent and Trademark Office

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Application Number: 10/678,936
Filing Date: October 03, 2003
Appellant(s): THOMAS ET AL.

Patrick C. Keane
Reg. No. 32,858
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 04/18/2008 appealing from the Office action mailed 09/18/2007.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,807,632	CARPENTIER et al.	10-2004
6,963,923	BENNETT	11-2005

Art Unit: 2132

7,242,766	LYLE	7-2007
2002/0076043	VAN DER VLEUTEN et al.	6-2002
2002/0107806	HIGASHI et al.	8-2002

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

Claims 1-4, 7, 28-31 and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Higashi et al. (2002/0107806) in view of Lyle (7,242,766).

Regarding claims 1-4 and 7 being representative of claims 28-31 and 34, Higashi specifically discloses a method comprising:

receiving a user's request to transfer a file (i.e., a request to purchase a content) (paragraphs 0012, 0100); locating the requested file stored in a memory (i.e., in a content database) (paragraph 0015);

computing a unique identifier corresponding to the requested file, (i.e., determining a content ID corresponding to the requested file, the content ID associating the requested file with content information such as usage rights and content encryption/decryption key) (paragraphs 0074-75, 0112, 0117);

choosing a first key K1, i.e., a content key (paragraph 0074);

encrypting K1, and the unique identifier with a second key K2, a public key, to generate a first value (i.e., encrypting content information LT including the content key and the content ID using the public key of the user such that the encrypted content

information LT can be decrypted later at the user's computer using the private key corresponding to the public key) (paragraphs 0080-0081, 0083, 0094, 0112, 0117);

encrypting the requested file with the first key, K1, to generate a second value (i.e., encrypting the requested content using the content key) (paragraphs 0086, 0128); and

transferring the first and second values (i.e., transferring the encrypted content information LT and encrypted content to the user's computer) (paragraphs 0087, 0094, 0128).

Higashi does not disclose that the encryption key K1 is unique to the particular transfer of the requested file. Lyle discloses a method for encrypting requested content wherein the encryption/decryption key (i.e., a session key) is unique to the particular transfer of the requested content (col. 22, lines 38-41). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Higashi method such that the encryption key K1 is unique to the particular transfer of the requested file, as taught by Lyle. Such an encryption/decryption key would vary from one transaction to the next.

Claims 5-6 and 32-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Higashi in view of Lyle as applied to claims 1 and 28 above, and further in view of Bennett (6,963,923).

Higashi does not disclose that interruption occurs to the transmission of the second value and when it happens, transmission of the second value will be resumed

without retransferring the entire second value. Bennett discloses that file transmission

interruptions do occur. Bennett also discloses a method for file transfer restart without

retransferring the entire file in the event of file transmission interruption (Abstract; col. 1,

lines 42-53). It would have been obvious to one of ordinary in the art at the time the

invention was made to incorporate Bennett method of file transfer restart in the event of

file transmission interruption into the combined method of Higashi and Lyle for file

transfer. The motivation for doing so would have been to avoid the need to retransfer

the entire file (Abstract).

Claims 8-10 and 35-37 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Higashi in view of Lyle as applied to claims 1 and 28, and further in

view of Carpentier et al. (6,807,632).

Higashi discloses that the unique identifier is the content ID. Higashi does not

disclose that the content ID is an MD5 checksum of the content. Carpentier discloses

using an MD5 checksum of content, i.e., a cryptographic hash binary sequence

identifier of digital content, as the content ID (Abstract; col. 8, line 32 – col. 9, line 20). It

would have been obvious to one of ordinary in the art at the time the invention was

made to modify the combined method of Higashi and Lyle to use an MD5 checksum of

content as the content ID, as taught by Carpentier. Not only such identifiers are human

readable and easily communicated for use, they can also be used to show conclusively

whether two digital contents are identical (col. 8, lines 57-65; col. 9, lines 4-15).

Claims 55-58 are rejected under 35 U.S.C. 103(a) as being unpatentable over Higashi in view of Lyle as applied to claims 1 and 28, and further in view of Van Der Vleuten et al. (2002/0076043).

Higashi does not disclose that the second value (the encrypted file) includes a plurality of versions of the requested file, each version differing in quality. Van Der Vleuten discloses scalably encoding content so that the encoded content includes multiple versions of the content, each version differing in quality (Abstract; paragraphs 0002-0003). It would have been obvious to one of ordinary in the art at the time the invention was made to modify the combined method of Higashi and Lyle to scalably encode the requested file so that the encoded file includes multiple versions of the file, each version differing in quality, as taught by Van Der Vleuten. Scalable encoding allows the same single bit stream simultaneously serves different channels with different capacities without the need to re-encode the original data.

(10) Response to Argument

a.   Appellant, on page 8, 1st paragraph, argues that neither of the documents [Higashi (US 2002/0107806) and Lyle (US 7,242,766)] teach or suggest using Appellants' claimed key K2 to encrypt a first key K1, having the features recited in claims 1 and 28.

The primary reference, Higashi, specifically discloses that two separate keys are utilized at the server side in the process of secure content delivering: a first key, K1, for encrypting the requested content (i.e., a content key) (paragraphs 0074, 0086); and a second key, K2, for encrypting the content information including the first key (i.e., using

the user's terminal ID or the user's public key to encrypt the content information including the content key, such that only the specific user's terminal or the private key corresponding to the public key can be used to decrypt the encrypted content information and retrieve the content key) (paragraphs 0080-0083, 0094). Thus, Higashi clearly discloses that the first key is encrypted by a second key such as the user's public key.

b.   Appellant, on page 8, 3rd paragraph, argues that the Lyle patent does not overcome the deficiencies of Higashi because Lyle merely suggests using a so-called "session key" to replace the public key of the first alternative when encrypting the content.

Lyle discloses using one of the following three keys as a content key for encrypting content: (i) a public key of the receiver so that the content can be decrypted using the receiver's private key, (ii) a symmetric key wherein the receiver can obtain the necessary key for decrypting the content, (iii) or a session key that varies from one transaction to the next (col. 22, lines 19-42). Therefore, Lyle suggests using the session key as the content key as opposed to using the public key or the symmetric key, which is similar to Higashi' content key.

c.   Appellant, from the last paragraph of page 8 through the 1st paragraph of page 9, argues that Lyle in combination with Higashi, at best, would only replace Lyle's session key with both the content key and the public key of Higashi.

Higashi utilizes two different keys for different purposes: a content key (the first key) for encrypting content, and a key-encrypting key (the second key) for encrypting

the content key. Therefore, Lyle's session key, which functions as a content key (i.e., it is used for encrypting content), only replaces Higashi's content key but not the key-encrypting key because the session key does not provide that functionality (i.e., it is not used for encrypting a content key).

d.   Appellant, from the last paragraph of page 8 through the 1st paragraph of page 9, argues that even if Lyle's session key is considered the claimed first key, neither Higashi nor Lyle teach or suggest encrypting such a key with the claimed second key.

The second key of claim 1 is used to encrypt the first key and the unique identifier. Claims 7 and 34 further recite that the second key is a public key. Attention is directed to Paragraph a above for the discussion of Higashi's content key being encrypted using the user's public key.

e.   Appellant, on page 9, 2nd paragraph, argues that the transfer of the requested file, as disclosed by the specification, remains valid over multiple transactions with different servers.

It is noted that the features upon which Appellant relies are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See In re Van Geuns, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/M. D./
Examiner, Art Unit 2132

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2132

Conferees:

/Benjamin E Lanier/
Primary Examiner, Art Unit 2132

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2132